Checklist: How Fortinet Helps DevOps Leaders Ensure Effective Security Without Slowing Cycles

Increased efficiency and reduced time to market are among the most important benefits of implementing DevOps processes and methodologies. In a recent survey of DevOps leaders, 56% reported that one of these two metrics was their number one success measurement.[1] However, speed and efficiency do not benefit an organization when it results in security events that impact operations and put the bottom line at risk. On the other hand, when reactive or tactical security measures are put in place to respond to these risks, they can lead to unacceptable—and unnecessary—delays.

7 Ways That Fortinet Streamlines DevSecOps

Fortinet helps DevOps teams keep their projects on track with an integrated security solution that eliminates the need for siloed point products and manual security processes.

Following are seven takeaways:

☑ Security integration.

The Fortinet Security Fabric integrates security solutions across the entire infrastructure—from on-premises to the cloud, and from traditional IT to DevOps environments. This eliminates security gaps that put the business at risk and slows DevOps cycles. The open ecosystem of the Fortinet Security Fabric helps Fabric-Ready Partners incorporate their solutions to meet DevOps-specific security needs. The Security Fabric also includes tools that enable transparent sharing of security information between the security operations and DevOps teams.

☑ Multi-cloud security services hub.

The FortiCASB-Cloud Public Cloud Guardian natively integrates security into major public cloud provider platforms to enable consistent control over all cloud resources—including infrastructures operated by DevOps teams across disparate clouds. It enables security teams to gain complete visibility across the diverse infrastructure while allowing application development teams to iterate rapidly without compromising security. FortiCASB-Cloud also identifies suspicious cloud activity or possible compromised accounts and alerts the DevOps and security teams.

☑ DevOps security from the ground up.

FortiGate next-generation firewalls (NGFWs) can support a perimeter-protection DevSecOps strategy with full automation capabilities that can be integrated into the DevOps continuous integration/continuous deployment (CI/CD) pipeline. This helps integrate application security protections and processes into DevOps projects from the ground up, rather than adding security protection as an afterthought or in a piecemeal fashion. Taking this approach also helps eliminate security-related delays associated with the integration of security into the software development life cycle.

☑ Cloud workload protection.

Applications being built in or migrated to the cloud need to be protected against new threats that propagate across workloads—and from cloud platform misconfigurations at the user interface (UI) and application programming interface (API) levels. Using FortiGate VM to secure traffic to and from the internet, and FortiCASB-Cloud to secure against risks associated with unwanted or unsupervised configurations at the cloud-account level, organizations can achieve a more reliable security posture in the cloud.

☑ Automated security and compliance process.

Given the speed at which DevOps cycles revolve, they cannot tolerate the change-controlled nature of manual security processes. The Fortinet Security Fabric offers scripts that enable the automation of many security aspects of the application life-cycle processes managed by DevOps teams, minimizing manual work and interruptions for both the security and DevOps teams.

☑ Intent-based integration.

Least privilege and information classification are fundamental information security principles. The need to classify information, services, and assets based on the role they play in an application's operational needs is common in the world of DevOps and agile development. This provides the flexibility for different developers to move at their own speed and the ability to track a consistent metadata-based information classification practice. By leveraging metadata and labels in security policies, a security infrastructure can enforce such separation of duties into an effective intent-based segmentation policy that carries through for both east-west and north-south traffic. This is enabled with cloud security services hubs powered by FortiGate VM.

☑ Container security.

When DevOps teams use application containers to make their applications more portable and resilient, they also introduce new security risks. A container security solution should address the needs for securing traffic into and across container clusters, securing container registries, and ultimately integrating security into the container-based application mesh as a containerized service. FortiGate VM NGFWs support awareness of container labels, the FortiWeb web application firewall is delivered as containers, and FortiSandbox can help mitigate risk associated with unsupervised use of container registries.

Simplify and Strengthen Network Defenses

The Fortinet Security Fabric helps DevOps organizations fully integrate security into their CI/CD pipeline while maintaining consistent security posture across the entire security infrastructure, both on-premises and across multiple clouds. This enables DevOps teams to focus on their projects rather than being distracted by security issues.

[1] "2019 State of DevOps Security Report," Fortinet, May 10, 2019.

FORTINET®

www.fortinet.com

June 6, 2019 1:06 AM

323490-0-0-EN

D:\Fortinet\Solution Brief\DevOps BOFU Checklist\FA - Checklist - DevOps BOFU